REMARKS

Claims 1 and 3-28 are all the claims presently pending in the application.

While Applicants believe that all of the claims are in condition for immediate allowance, to speed prosecution, claim 1 is amended herewith to include the features of dependent claim 2 to define more clearly and particularly the features of the present invention. Claim 2 correspondingly is canceled without prejudice or disclaimer.

New claim 28 is added to provide more varied protection for the present invention.

It is noted that the claim amendments are made only for more particularly pointing out the invention, and not for distinguishing the invention over the prior art, narrowing the claims or for any statutory requirements of patentability. Further, Applicants specifically state that no amendment to any claim herein should be construed as a disclaimer of any interest in or right to an equivalent of any element or feature of the amended claim.

Claims 1-27 stand rejected on prior art grounds. Particularly, claims 1, 3-6, 24, 25, and 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Urata (U.S. Patent No. 6,799,272) in view of Kawan (U.S. Patent No. 6,289,324). Claims 8, 15-18, and 20-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Urata in view of Kawan, and further in view of Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Second Edition, pps. 466-474 (hereinafter, "Schneier"). Claims 2, 10-12, 14, 23, and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Urata in view of Kawan, and further in view of Perlman et al. (U.S. Patent No. 5,261,002; hereinafter "Perlman"). Claim 19 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Urata in view of Kawan, and further in view of Schneier, and further in view of Perlman.

These rejections are respectfully traversed in the following discussion.

I. THE CLAIMED INVENTION

In conventional methods and systems, counterfeiting/duplication is not rendered difficult since confidential information is carried on the card and an unscrupulous person may find the information simply by looking at or reading the energy construction inside of the card. That is, with a plurality of readings of the card, the information held within the card can be easily detected (e.g., see specification at page 3, line 19, to page 4, line 2).

The claimed invention, on the other hand, complements the conventional smart-card-type of security, which is often all carried on the card itself, by providing extra protection depending on cryptography, with the cryptographic structure (e.g., a key) not being carried by the card and which cannot be accessed completely by a predetermined small number of readings. Moreover, the cryptographic structure can only be built by whoever emits the card or the agent thereof (e.g., see specification at page 4, lines 9-13).

The claimed invention, in addition to preventing the creation of false cards different from the legitimate ones, also prevents the fabrication of clones of a given legitimate smart card. That is, the present invention also provides a mechanism of protection designed to prevent and/or discourage both copying and creation of new cards (e.g., see specification at page 4, lines 14-17).

For example, in an illustrative, non-limiting embodiment of the invention, as defined by independent claim 1, a method of preventing counterfeiting of a smart card includes providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined small number of readings, wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof. The method further includes providing a reader for reading the smart card and including a database holding

information related to unauthorized smart cards. The reader is on-line, such that the reader is operatively connected to a network, only when the database of the reader is being updated by the network.

II. THE PRIOR ART REJECTIONS

A. Urata (U.S. Patent No. 6,799,272)

Urata relates to a method and system for authenticating a remote device. Particularly, Urata discloses that a remote device and an authentication center each store an identical key code index which includes a plurality of key code numbers. The remote device and authentication center communicate with each other through first and second keys, that each specify a particular key code number from the key code index.

Specifically, the remote device translates the first key received from the authentication center to determine the particular key code number and then generates a second key also specifying the particular key code number. Thereafter, the authentication center translates the second key to determine a second key code and compares the first and second key code numbers. If the two key code numbers match, the remote device is authenticated.

The remote device may be, for example, (1) a wireless telephone, (2) a smartcard or (3) a credit card used in conjunction with an Internet access device such as a personal computer (PC) and the authentication center may be, for example, a wireless base station or a credit/smartcard authentication center (e.g., see Urata at column 2, lines 31-52).

B. Kawan (U.S. Patent No. 6,289,324)

Kawan relates to a financial information and transaction system comprising a host financial computer system, which maintains records of user account information, and at least one terminal providing a user interface for accessing the host financial computer system. The terminal includes a means for transmitting and receiving data corresponding to the user account information, and a smart card interface device.

Kawan discloses that a financial information and transaction system includes a host financial computer system, which maintains records of user account information, and at least one terminal providing a user interface for accessing the host financial computer system.

The terminal includes a means for conducting a transaction based on the user account information, a smart card interface device, and a smart card (e.g., see Kawan at Abstract).

Kawan discloses that encryption and decryption, also called ciphering and deciphering, prevent someone from counterfeiting a smart card as long as the encryption keys are known only to the issuer of the smart card and the entity supporting the ATM and merchant terminal system. If the smart card's result is the same string with which the ATM or merchant terminal started, the smart card is authenticated and the desired transaction may proceed (e.g., see Kawan at column 9, lines 36-43).

C. Perlman et al. (U.S. Patent No. 5,261,002)

Perlman relates to a technique for issuing and revoking user certificates of authenticity in a public key cryptography system, wherein certificates do not need expiration dates, and the inconvenience and overhead associated with routine certificate renewals are minimized or avoided entirely (e.g., see Perlman at Abstract).

To deal with authentication problems, Perlman discloses that many systems use authentication certificates. Perlman discloses that **the basic function of authentication certificates is to vouch for the relationship between a public key and the person or entity to which it belongs**. Perlman defines a "certificate" as a cryptographically signed message indicating that a trusted authority vouches for the relationship between a public key and a named principal or owner of the key. Each certificate is "signed" by the trusted authority, known as the Certification Authority, to ensure authenticity of the certificate itself. Certificates may be held by their owners, who present copies to other users with whom they wish to communicate, or may be posted in a public place. The certificates may also employ a public key cryptography system to produce digital signatures, but this need not necessarily be the same system as the one for which keys are being published.

For complete network security, every user must have a certificate. Sometimes, however, it is necessary to invalidate certificates; for example, when an employee is fired or transferred, or when a password falls into the wrong hands. There are two common mechanisms for accomplishing this: (1) issuing certificates with expiration dates that define relatively short validity periods, and (2) establishing a "blacklist" of invalid certificates (e.g., see Perlman at column 2, lines 28-68).

With respect to (2) above, Perlman discloses that the Certification Authority issues a signed "blacklist" periodically or on demand, containing a list of the certificates that have been issued in the past, but which are now to be considered invalid. Since the blacklist will normally be short, it can be issued with much greater frequency than the individual certificates. Anyone who wishes to verify that a certificate is valid must first check that the certificate has not expired,

and then that the certificate is not included in a current blacklist issued by the Certification Authority (e.g., see Perlman at column 3, lines 1-40).

To allegedly improve over the related art described in Perlman above, Perlman discloses a method for authenticating users of an information system and, more specifically, users of a public key cryptography system. In the method described by Perlman, certificates are not required to have an expiration date, so much of the inconvenience of periodic certificate renewals is avoided. Instead, a blacklist has a start date and an expiration date, and any certificates issued prior to the start date are automatically considered invalid.

The Perlman method includes a first step of issuing a signed certificate for each user of the system, wherein the signed certificate contains an issue date and any other desired public information pertaining to the user, such as a public key, issuing a signed blacklist containing a blacklist start date, a blacklist expiration date, and an entry for each user whose certificate was issued after the blacklist start time and is to be considered invalid. Perlman then discloses a second step of determining whether a user's certificate is valid by first obtaining a copy of the certificate and a copy of the signed blacklist, then determining whether the certificate issued after the blacklist start date and is not on the blacklist, in which case the certificate is presumed to be valid (e.g., see Perlman at column 3, lines 64-68, and column 4, lines 1-18).

Thus, Perlman relates to authentication certificates that do not require expiration dates, thereby avoiding the inconvenience and overhead associated with frequent certificate renewals. When the blacklist becomes too long, it can be shortened by choosing a new blacklist start date, and issuing renewed certificates to replace old valid certificates issued prior to the new blacklist start date.

Perlman states that the principal advantage of the invention is that certificates must be issued only when the blacklist gets too long. In the prior art, certificates must be issued periodically, where the period is determined by the time in which the blacklist might get too long (e.g., see Perlman at column 4, lines 63-68, and column 5, lines 1-10).

D. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Second Edition, pps. 466-474.

Schneier is a treatise on public-key algorithms.

E. Response to Examiner's Position

The Examiner alleges that the claimed invention would have been obvious over various combinations of Urata, Kawan, Perlman, and Schneier.

Applicants respectfully submit, however, that it would not have been obvious to combine Urata, Kawan, Perlman, and Schneier, either individually or in combination, to in order to arrive at the claimed invention. Moreover, Applicants submit that, even assuming *arguendo* that it would have been obvious to combine these references, there are elements of the claimed combination which are not disclosed or suggested by Urata, Kawan, Perlman, and Schneier, either individually or in combination. Therefore, Applicants respectfully traverse these rejections.

As mentioned above, Urata discloses that a remote device and an authentication center each store an identical key code index which includes a plurality of key code numbers. The remote device and authentication center communicate with each other through first and second

keys, that each specify a particular key code number from the key code index, to authenticate the remote device, which may be a smartcard (e.g., see Urata at column 2, lines 31-52).

On the other hand, Kawan discloses that encryption and decryption, also called ciphering and deciphering, prevent someone from counterfeiting a smart card as long as the encryption keys are known only to the issuer of the smart card and the entity supporting the ATM and merchant terminal system (e.g., see Kawan at column 9, lines 36-43).

The Examiner acknowledges that Urata and Kawan do not disclose or suggest "*a data base holding information related to unauthorized smart cards, said reader being on-line, such that said reader is operatively connected to a network, only when said database of said reader is being updated by said network*" (see Office Action at page 10, lines 6-10).

However, the Examiner alleges that Perlman makes up for the deficiencies of Urata and Kawan by allegedly disclosing "*a data base holding information related to unauthorized smart cards, said reader being on-line, such that said reader is operatively connected to a network, only when said database of said reader is being updated by said network (col. 3, lines 38-40, col. 6, lines 37-39, and fig. 1, ref. num 24-30)*" (see Office Action at page 10, lines 11-14). The Examiner alleges that it would have been obvious to combine Urata, Kawan, and Perlman "*because the off-line version of the blacklist provides a listing of all users who are intruders; the periodic updating allows a newer list of intruders to be known*" (see Office Action at page 11, lines 1-4).

Applicants respectfully submit, however, that Perlman does not make up for the deficiencies of Urata and/or Kawan. Instead, Perlman merely discloses a "blacklist" for certificates of authenticity in which the certificates do not need expiration dates (e.g., see Perlman at Abstract).

Perlman does not disclose or suggest the novel and unobvious combination of elements as defined by the claimed invention, including "*providing a reader for reading said smart card and including a database holding information related to unauthorized smart cards, said reader being on-line, such that said reader is operatively connected to a network, only when said database of said reader is being updated by said network*", as defined by independent claim 1.

Applicants note that the references as a whole must be considered for what they fairly teach to the ordinarily skilled artisan. Moreover, merely identifying individual elements of the claims in separate references is not sufficient to establish the obviousness of the claims. The Office Action must establish a reasonable motivation or suggestion, in the references themselves or in the art in general, for combining the references to arrive at the claimed invention.

Indeed, Applicants note that, the mere fact that references could (or can) be combined or modified is not sufficient to establish *prima facie* obviousness (see M.P.E.P. § 2143.01). There must be a reasonable motivation, in the references themselves or in the art in general, to do that which the patent Applicants have done.

Applicants respectfully submit that (at best) the alleged combination of the cited references would be a smart card which uses the cryptographic schemes of Kawan to protect secret information or messages on the smart card of Urata, in which the user or owner of the smart card is issued an authentication certificate to vouch for the relationship between a public key and the person or entity to which it belongs (e.g., see Perlman at column 2, lines 37-41).

However, this resulting combination merely is comparable to conventional cryptographic schemes used with smart cards to protect the confidential information on the smart card and the use of authentication certificates as described by Perlman to confirm that the relationship

between a public key and the named principal or owner of the key (e.g., see Perlman at column 2, lines 37-41).

In fact, the **Perlman reference itself specifically contemplates "*smart cards*"** (e.g., see Perlman at column 3, lines 13-16), but does **not** disclose or suggest the claimed combination of "*providing a smart card*" and "*providing a reader for reading said smart card and including a database holding information related to unauthorized smart cards, said reader being on-line, such that said reader is operatively connected to a network, only when said database of said reader is being updated by said network*", as defined by claim 1 of the present invention.

Thus, Applicants submit that the claimed invention clearly would not have been obvious from any combination of Urata, Kawan, Perlman, and Schneier, either individually or in combination.

In stark contrast to the cited references (or alleged combination thereof), the present invention provides a novel and unobvious method of preventing counterfeiting (i.e., false smart cards or illegitimate cards) and/or preventing cloning (i.e., copies of legitimate smart cards or counterfeit smart cards) of a smart card by authorizing (e.g., verifying the legitimacy of) the smart card. That is, the claimed invention provides a simple and effective solution to problems with conventional smart cards which use cryptographic schemes merely to protect secret information or messages on the smart card itself, but do not authorize or authenticate a smart card (i.e., do not prevent counterfeiting and cloning of a smart card).

Thus, Applicants respectfully submit that Urata, Kawan, Perlman, and Schneier, either individually or in combination, do not disclose or suggest all of the features of the novel and unobvious combination of elements of the claimed invention, as recited in claim 1. Therefore,

Applicants further submit that the alleged combination of references, even if combined in the manner alleged by the Examiner, would not arrive at the claimed invention.

Applicants respectfully submit that Schneier does not make up for the deficiencies of Urata, Kawan, and Perlman, as set forth above.

Therefore, Applicants submit that all of the pending claims (i.e., claims 1 and 3-27) are patentable over Urata, Kawan, Perlman, and Schneier, either individually or in combination, for somewhat similar reasons as those set forth above with respect to independent claim 1.

Therefore, Applicants respectfully request that the Examiner withdraw the rejections and permit claims 1 and 3-27 to pass to immediate allowance.

III. NEW CLAIM

New claim 28 is added to provide more varied protection for the present invention.

Applicants submit that new claim 28 is patentable over the cited references for somewhat similar reasons as those set forth above, as well as for the additional features recited therein.

IV. CONCLUSION

In view of the foregoing, Applicants submit that claims 1 and 3-28, all the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: June 9, 2005

John J. Dresch, Esq.
Registration No. 46,672
Sean M. McGinn, Esq.
Registration No. 34,386

McGinn & Gibb, PLLC
8321 Old Courthouse Road, Suite 200
Vienna, VA 22182-3817
(703) 761-4100
Customer No. 21254

CERTIFICATE OF TRANSMISSION

I certify that I transmitted via facsimile to (703) 872-9306 the enclosed Amendment under 37 C.F.R. § 1.111 to Examiner Brandon S. Hoffman on June 9, 2005.

John J. Dresch, Esq.
Registration No. 46,672
Sean M. McGinn, Esq.
Registration No. 34,386